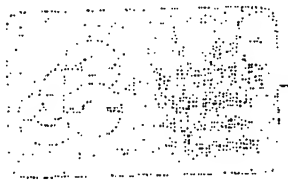
Appendix A

The AIRMAGNET

Distributed WLAN Integrity Management System

The past year has seen the role of the Wireless LAN in the enterprise undergo a fundamental transformation. A groundswell of demand from both CXOs and end-users alike has made Wi-Fi a pervasive component of the enterprise network. This adoption, however, has been anything but strict. Growth has been notoriously viral and unregulated, making it a challenge to even know about all the Wi-Fi infrastructure being deployed, much less manage it.

New breeds of security measures have evolved out of necessity, but have done so without a methodology to insure that they are actually enforced. Environmental factors continue to impact the performance and reliability of the network itself, and a reliance on outdated tools intended for wired networks has forced network managers into a purely reactive management strategy. These issues are the unique domain of the AirMagnet Distributed System.

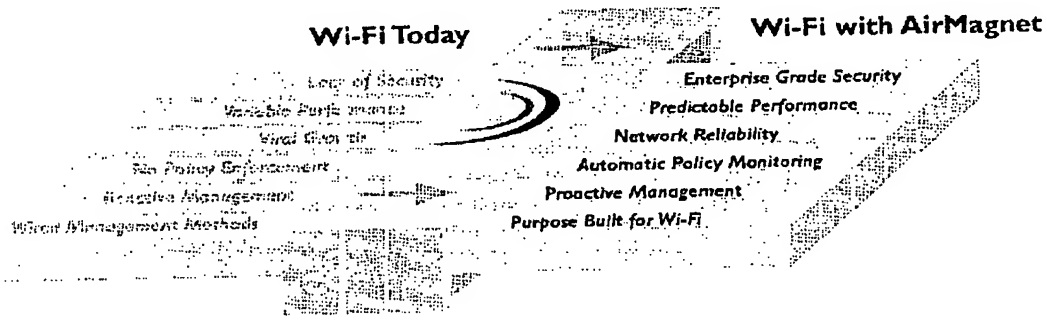


WLAN Integrity Management ensuring network Security Performance and Reliability

The AirMagnet Distributed System

The AirMagnet Distributed System is the first and only solution to fully address the Integrity of wireless networks - providing 24x7 monitoring of the Security, Performance, and Reliability of any number of WLANs, and delivering actionable information to management staffs and systems anywhere in the world.

AirMagnet Distributed replaces an informational void with complete knowledge of every Wi-Fi device and channel in the environment regardless of band (11a, 11b, or 11g). Management staff can easily monitor the security measures in use on every device to insure compliance with established policies, while automatically scanning for dozens of wireless network attacks. In addition to security, the AirMagnet Distributed System proactively addresses the performance and reliability of the network, without which, the WLAN simply could not be held to enterprise standards. Dozens of configurable alarms proactively alert managers to developing issues before they lead to problems, and a suite of active testing utilities enable managers to test their infrastructure from any location they choose.



AirMagnet Distributed

WLAN Integrity Management delivers security, performance, and reliability throughout the network lifecycle

AirMagnet Distributed: The Industry's Most Sophisticated Monitoring

The front line of the AirMagnet Distributed System is manned by strategically placed Intelligent Sensors. These sensors provide around-the-clock coverage of the entire wireless environment including all 11a, 11b, and 11g channels and infrastructure. Each individual sensor is armed with the patent-pending AirWISE Analytical Engine, to autonomously monitor the security, performance, and reliability of the network. Functionality built into each sensor, allows network professionals to:

Gain Control Over Security Policy

No issue has defined Wi-Fi more than security. While the past year has welcomed new security protocols that make WLANs as secure as their wired counterparts, insuring that all users and stations comply with these security measures has been another issue entirely. AirMagnet Sensors address this gap by auditing and validating the security of every Wi-Fi device in the network, providing managers with an easy process to insure all users employ the appropriate level of security. Supported protocols include:

- wep
- leap
- peap
- tkip
- mic
- 802.1x
- ttls
- tls
- wpa
- pptp vpn
- l2tp vpn
- ssh vpn
- ipsec vpn

Detect Wireless Intruders and Attacks

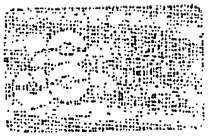
Maintaining internal defenses is only half the security battle. As Wi-Fi has grown, so too have the number and sophistication of wireless attacks. AirMagnet Sensors have been engineered specifically to counter these threats - scanning the environment for Rogue APs and War-Drivers, Spoofed MAC Addresses, and a host of Denial of Service Attacks unique to Wi-Fi. Sensors send encrypted real-time alarms in response to an attack , allowing staff to respond before the network is impacted.

Lock In Network Performance

Radio Frequency transmissions are inherently susceptible to environmental factors such as physical obstructions and radio interference from a variety of sources. If not identified and managed, these factors can lead to unacceptable performance for the end-user. To address this challenge, AirMagnet Sensors constantly monitor and alarm on over 20 key indicators of network health, allowing engineers to take a proactive approach to the maintenance of the network.

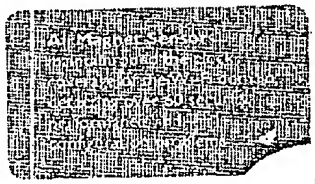
Ensure Network Reliability

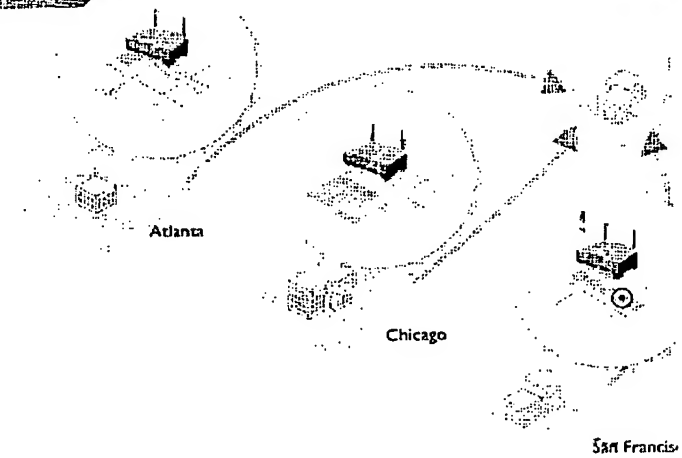
In addition to predictable performance, WLANs must be highly reliable before being considered business grade. The AirMagnet Distributed System addresses this need with a suite of alarms and diagnostics that detect network faults and misconfigurations that can lead to outages in the network. These diagnostics are complemented by active utilities to pin down the sources of connectivity problems in the network.

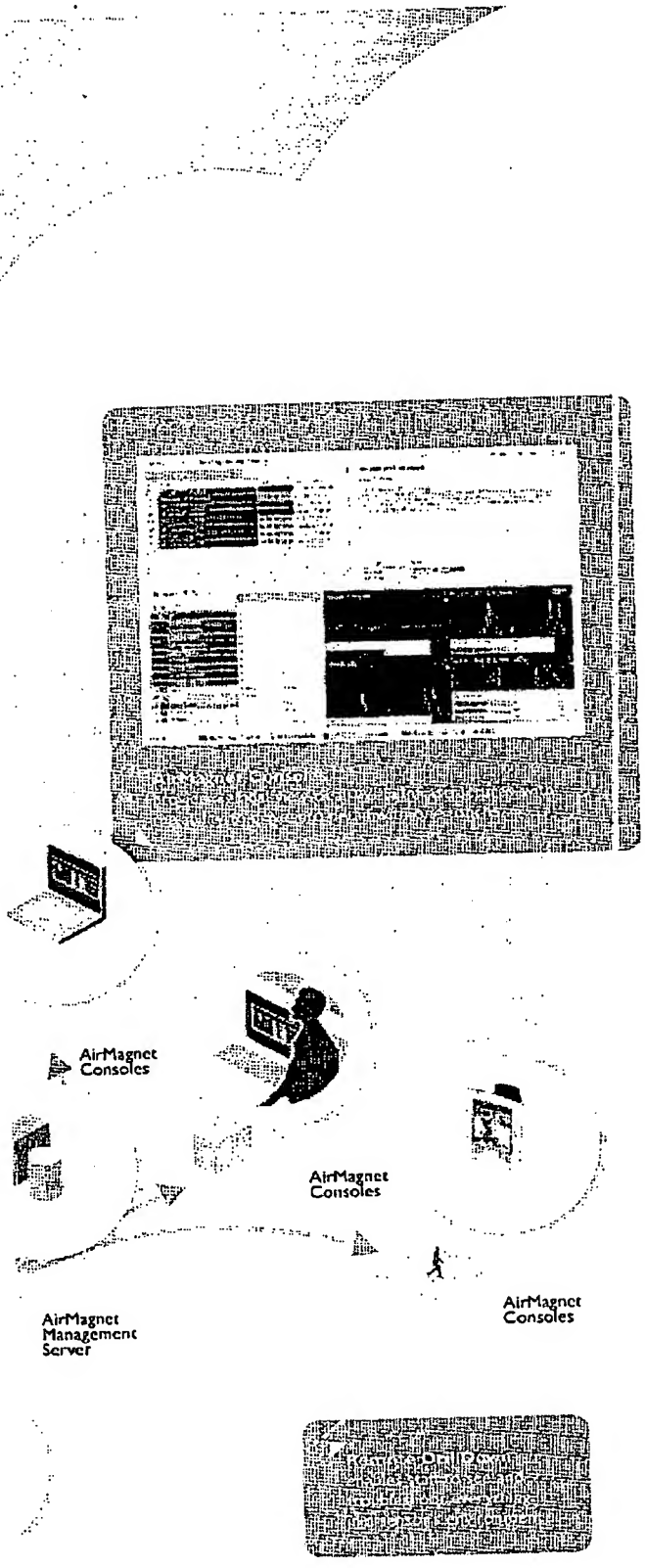


AirMagnet Distributed: 24x7 Wi-Fi Integrity Management

- multi-band coverage - 11 a,b,g
- infrastructure agnostic
- standards based security
- control over network policy and growth
- proactive management
- local processing ensures enterprise scalability
- integrated with leading network management consoles







Secure Scalable Management

Controlled Centralized System Management

The AirMagnet Management Server receives information from every AirMagnet Sensor and provides a centralized SQL database of all network data and alarms. SNMP traps allow for seemless integration with leading management consoles such as HP Open View and CA UniCenter. All traffic is secured via SSL and TLS insuring management information remains secure while interoperating with corporate firewalls and VPNs.

Configuration and User Management

The Management Server also maintains configurations for every Sensor in the System, allowing IT Personnel to tune sensor thresholds appropriately for each location. Additionally, AirMagnet Distributed supports three unique user levels, insuring that the users access only the level of information appropriate for their role and level of responsibility.

Anywhere, Anytime Integrity Management

The AirMagnet Management Console provides the User Interface to The AirMagnet Distributed System. From the Management Console, Users can view alarms and WLAN health by Campus, Building, Floor, or by individual Sensor. Consoles can be run securely whether in a NOC, or remotely on a laptop or Pocket PC - keeping networkers connected to the information they need, regardless of their location.

Remote Drill-Down

One of the most powerful features of the AirMagnet Console is the ability to remotely drill in to any AirMagnet Sensor. This allows Users to securely connect to a particular sensor, from any location, and view detailed information in real-time. Users can view low level data on every channel and device in the area, see alarms, real-time local statistics, and even review packet decodes.

Remote Troubleshooting and Active Tools

Using the Remote UI built into the AirMagnet Management Console, Users can leverage a host of active troubleshooting tools to pinpoint problems in the network. These tools allow the User to remotely test Throughput on a particular AP, Diagnose Connection Problems, and perform Layer 3 Debugging and End-to-End Provisioning. Such remote capability greatly reduces the need to dispatch resources when troubleshooting the WLAN.

Efficient Use of Network Resources

Most remote monitoring systems simply capture wireless packets and resend them to a remote site for processing, needlessly consuming valuable bandwidth. AirMagnet Sensors, conversely process locally, sending real-time alarms only when thresholds are reached. Trending data is saved on the sensor, and securely sent at regular intervals to the Management Server, minimizing operational load on the network and servers.

The Comprehensive Solution

AirMagnet Distributed Specifications

General

Supported 802.11 Standards	A, B, G
Radio Frequency	2.4 GHz, 5 GHz Bands Concurrently
Supported Security Standards	802.1x, LEAP, TKIP, MIC, PEAP, WPA, VPNs
SNMP Traps	Yes
Integration to 3rd Party Consoles	HP OpenView, CA Unicenter
Reporter Option	Yes
Secure Communication	SSL, TLS
Real-Time Decode	Yes
Decode Level	Layers 1,2,3
Trace File Compatibility	AirMagnet, Sniffer, Ethereal

Security Management

Policy Enforcement - Detects 15 Violations

- AP with WEP Disabled
- Client Station with WEP Disabled
- WEP IV Reused
- Device Using Open Authentication
- AP Unconfigured
- Rogue AP
- Rogue Client Station
- Crackable WEP IV In Use
- Device Unprotected by VPN
- Device Unprotected by 802.1x
- AP Broadcasting SSID
- Ad-hoc Station Detected
- Long EAPRekey Timeout
- Device Using Shared Key Authentication
- Unassociated Station Detected

Intrusion Detection - Detects 16 Threats

- Spoofed MAC Address Detected
- Device Probing With NULL SSID
- Dictionary Attack in EAP Methods
- Abnormal Authentication Failures
- Denial of Service Attacks
  - Association Flood
  - Authentication Flood
  - EAPOL logoff
  - EAPOL start
  - EAPOL ID Flood
  - EAPOL Spoofed Success
  - Deauthentication Broadcast
  - Deauthentication Flood
  - Dis-association Broadcast
  - Dis-association Flood
  - RF Jamming

AirMagnet, Inc.
465 Fairchild Drive,
Suite 203
Mountain View, CA
94043
650-694-6754
www.AirMagnet.com
info@airmagnet.com

End to End Connectivity

- Mismatched SSID
- Client with Match All SSID
- Mismatched RF Channel
- Mismatched Privacy Setting
- Authentication Failure
- Reassociation Failure
- Possible Equipment Failure
- AP Signal Out of Range
- Mismatched Capability Settings
- Device With Bad WEP Key
- Higher Layer Protocol Problem
- 802.1x Authentication Failure

Tools

- Perform
  - Ping
  - DHCP
  - TraceRoute
  - Whois

Performance Management

Detects 12 Sources of Poor Performance

- AP With Weak Signal Strength
- Low Transmission Speed
- High Packet Fragmentation Rate
- High Bandwith Usage
- Missed AP Beacons
- High Speed Transmission Not Supported
- Channel Overloaded by APs
- 802.11 Performance Options Not Supported
- APs With Mutual Interference
- High Mgmt and Control Frame Overhead
- AP Overloaded with Clients
- AP Overloaded by Bandwith Consumption

Reliability Management

Detects 13 Sources of Poor Reliability

- WLAN Hidden Node Problem
- AP System of Firmware Reset
- Station Excessively Switching Between APs
- Packet Error Rate Exceeded
- AP Association Capacity Full
- Channel with Overloaded APs
- DCF and PCF Controls Active at Same Time
- Conflicting AP Configuration
- Channel with High Noise Levels
- High Multicast/Broadcast Traffic
- Ad-hoc Station Using AP SSID
- Station Constantly Probing for Connection

Software Sensor

Operating System	Windows 2000, XP (PC Not Included)
Memory	128 MB Minimum
Disk Storage	20 MB Free Space Minimum
Supported 802.11 PC or PCI Cards	Cisco PCM352, LMC352, PCI352, NetGear WAB501

Appliance Sensor

Operating System	Embedded Linux (Hardware Included)
Memory	64 MB
Antenna	Omni-directional, 2.4 GHz: 3.0 dbi, 5.25 GHz: 5.5 dbi, 5.75 GHz: 5.8 dbi
802.11 Radio Card	Atheros based a/b/g multi-mode card
10/100 Ethernet Port	2 With Power Over Ethernet Option

Management Server

Operating System	Windows 2000, XP (PC Not Included)
CPU	800MHz Minimum
Memory	256 MB Minimum
Disk Storage	4 GB Free Space
# Of Sensors Supported	Unlimited
Information Repository	Aggregate Sensor Alarms, wireless device and traffic trends

Management Console

Operating System	Windows 2000, XP (PC Not Included)
CPU	800 MHz Minimum
Memory	256 MB Minimum
Disk Storage	20 MB Free Space Minimum

AIRMAGNET